

Ingress Controller Risks

New tools can introduce risks that might outweigh the rewards. Here are the top three risks that can be introduced by an Ingress controller that doesn't align to your needs.

01

Complexity

Does it Defeat the Purpose of a Microservices Architecture?

Complexity is one of the top challenges in using and deploying containers.¹

The wrong Ingress controller can add even more complexity – limiting your ability to scale the deployment horizontally and negatively impacting app performance.

02

Latency

Does the Ingress Controller Slow Down Your Apps?

Organizations adopt Kubernetes for the ability to deploy new apps more quickly.²

But an Ingress controller that adds latency through errors, timeouts, and reloads can slow down your apps.

03

Security

Does the Ingress Controller Open the Door for Hackers?

More than half of organizations have delayed or slowed down application deployment into production due to container or Kubernetes security concerns.³

Watch out for Ingress controllers with slow CVE patching and beware of relying on support from public forums.

Click here to learn more at nginx.com



¹ CNCF Survey 2020

² 2021 Kubernetes Adoption Survey

³ Red Hat State of Kubernetes Security Report